WHAT IS CLAIMED IS:

1. A method for using a utility at an end user device, comprising:

assigning an elevated access right to a remote user identifier and a limited access right to an end user identifier, the limited access right operable to prevent access to the utility at the end user device;

accessing the utility at the end user device using the remote user identifier, the utility operable to allow the remote user identifier to select an administrative tool at the end user device;

launching the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier; and

performing at least one administrative task at the end user device using the administrative tool.

2. The method of Claim 1, wherein assigning an elevated access right to a remote user identifier and a limited access right to an end user identifier further comprises:

setting up at a network directory a remote user profile for the remote user identifier, the remote user profile associating the remote user identifier with the elevated access right; and

setting up at the network directory an end user profile, the end user profile associating the end user identifier with the limited access right.

3. The method of Claim 1, wherein accessing the utility at the end user device using the remote user identifier further comprises

receiving the remote user identifier;

authenticating the remote user identifier using a network directory, the network directory comprising a profile associating the remote user identifier with the elevated access right; and

granting access to the utility using the elevated access right.

4. The method of Claim 1, further comprising establishing a remote connection using a remote control module at a remote user device.

5. The method of Claim 4, further comprising:

detecting a break in the remote connection; and

closing at least one process, the at least one process corresponding to the administrative tool used to perform the administrative task.

6. The method of Claim 1, wherein the remote user identifier is associated with the remote user device, the remote user device located at a separate location from the end user device.

7. The method of Claim 1, wherein the administrative task comprises operations that affect the settings of the end user device.

8. The method of Claim 1, wherein the end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000.

9. A method of elevating an access right at an end user device, comprising:

receiving an authentication message from a network in response to a login request from a remote user identifier, the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device;

generating an elevated access layer using the elevated access right, the elevated access layer operable to:

initiate an administrative tool at the end user device; and

elevate the access right of the remote user identifier according to the elevated access right;

launching the administrative tool using the elevated access layer; and

processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right, the limited access right operable to prevent access to the administrative tool at the end user device.

10. The method of Claim 9, further comprising detecting a remote connection from the remote user device, the remote connection operable to access the end user device using a remote control module at the remote user device.

11. The method of Claim 10, further comprising discontinuing at least one process associated with the administrative tool upon detecting a break in the remote connection.

12. The method of Claim 9, wherein the remote user identifier is associated with a remote user device, the remote user device being at a separate location from the end user device.

13. A system for elevating access rights of a remote user, comprising:

a network directory operable to assign an elevated access right to a remote user identifier and a limited access right to an end user identifier;

a utility stored at an end user device and operable to:

launch the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier, the limited access right operable to prevent access to the utility at an end user device; and

perform at least one administrative task at the end user device using the administrative tool; and

a remote user device operable to access the utility at the end user device using the remote user identifier in order to perform the at least one administrative task at the end user device.

14. The system of Claim 13, the network directory further operable to:

set up a remote user profile for the remote user identifier, the remote user profile associating the remote user identifier with the elevated access right; and

set up an end user profile, the end user profile associating the end user identifier with the limited access right.

15. The system of Claim 13, the utility further operable to:

receive the remote user identifier;

authenticate the remote user identifier using a network directory, the network directory comprising a profile associating the remote user identifier with the elevated access right; and

granting access to the administrative tool using the elevated access right.

16. The system of Claim 13, the remote user device further operable to establish a remote connection using a remote control module.

17. The system of Claim 16, the utility further operable to:

detect a break in the remote connection; and

close at least one process, the at least one process corresponding to the administrative tool used to perform the administrative task.

18. The system of Claim 13, wherein the remote user identifier is associated with the remote user device, the remote user device located at a separate location from the end user device.

19. The system of Claim 13, wherein the administrative task comprises operations that affect the settings of the end user device.

20. The system of Claim 13, wherein the end user device comprises an operating system selected from a group consisting of WINDOWS XP and WINDOWS 2000.

21. Software for elevating an access right at an end user device, the software embodied in a computer medium and operable to:

receive an authentication message from a network in response to a login request from a remote user identifier, the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device;

generate an elevated access layer using the elevated access right, the elevated access layer operable to:

initiate an administrative tool at the end user device; and

elevate the access right of the remote user identifier according to the elevated access right;

launch the administrative tool using the elevated access layer; and

process at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right, the limited access right operable to prevent access to the administrative tool at the end user device.

22. The software of Claim 21, further operable to detect a remote connection from the remote user device, the remote connection operable to access the end user device using a remote control module at the remote user device.

23. The software of Claim 21, further operable to discontinue at least one process associated with the administrative tool upon detecting a break in the remote connection.

24. The software of Claim 21, wherein the remote user identifier is associated with a remote user device, the remote user device being at a separate location from the end user device.

25. A system for using a utility at an end user device, comprising:

means for assigning an elevated access right to a remote user identifier and a limited access right to an end user identifier, the limited access right operable to prevent access to the utility at the end user device;

means for accessing the utility at the end user device using the remote user identifier, the utility operable to allow the remote user identifier to select an administrative tool at the end user device;

means for launching the administrative tool according to the elevated access right while maintaining the limited access right of the end user identifier; and

means for performing at least one administrative task at the end user device using the administrative tool.

26. A system for elevating an access right at an end user device, comprising:

means for receiving an authentication message from a network in response to a login request from a remote user identifier, the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device;

means for generating an elevated access layer using the elevated access right, the elevated access layer operable to:

initiate an administrative tool at the end user device; and

elevate the access right of the remote user identifier according to the elevated access right;

means for launching the administrative tool using the elevated access layer; and

means for processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right, the limited access right operable to prevent access to the administrative tool at the end user device.

27. A method of elevating an access right at an end user device, comprising:

receiving an authentication message from a network in response to a login request from a remote user identifier, the authentication message operable to inform if the remote user identifier is associated with an elevated access right, the elevated access right operable to allow access to an administrative tool at the end user device, the remote user identifier associated with a remote user device, the remote user device being at a separate location from the end user device;

generating an elevated access layer using the elevated access right, the elevated access layer operable to:

initiate an administrative tool at the end user device; and

elevate the access right of the remote user identifier according to the elevated access right;

launching the administrative tool using the elevated access layer; and

processing at least one administrative task at the end user device using the administrative tool while maintaining an end user identifier logged into the network with a limited access right, the limited access right operable to prevent access to the administrative tool at the end user device;

detecting a remote connection from the remote user device, the remote connection operable to access the end user device using a remote control module at the remote user device; and

discontinuing at least one process associated with the administrative tool upon detecting a break in the remote connection.